PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-163235
(43)Date of publication of application : 07.06.2002

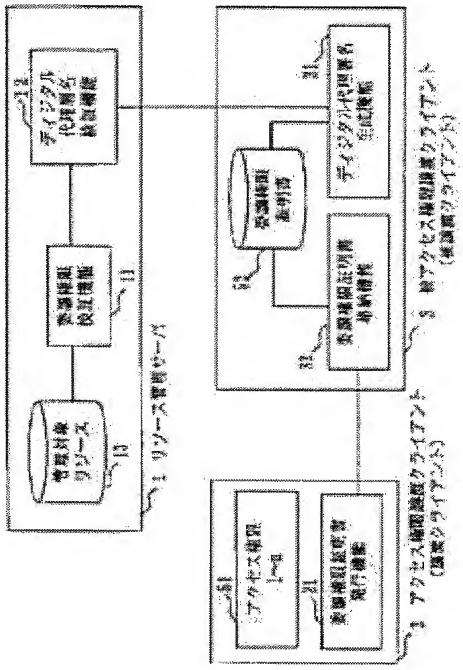
(51)Int.Cl. G06F 15/00

(21)Application number : 2000-361571
(22)Date of filing : 28.11.2000

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : NAKANO HATSUMI
NAKAKAWAJI TETSUO

(54) ACCESS AUTHORIZATION TRANSFER DEVICE, SHARED RESOURCE MANAGEMENT SYSTEM AND ACCESS AUTHORIZATION SETTING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To easily realize assignment of a temporary access authorization and assignment of a specified type of access authorization to a device without access authorization to a hared resource.
SOLUTION: A transfer client 2 issues an assignment authorization certificate 52 certificating temporary or definite transfer of access authorization to a management subject resource 13 by using an assignment authorization certificate issuing function 21, a transferred client 3 obtains the assignment authorization certificate 52 through an assignment authorization certificate storing function 32, and generates a digital agent signature which is an access request according to the obtained assignment authorization certificate 52 by a digital agent signature generating function 31. A resource management server 1 receives the digital agent signature, and verifies whether an access to the management subject resource by the transferred client 3 is properly requested or not through the digital agent signature verifying function 12 and an assignment authorization verifying function 11.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－163235
（P2002－163235A）
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｄ　５Ｂ０８５

審査請求　未請求　請求項の数16　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－361571(P2000－361571)

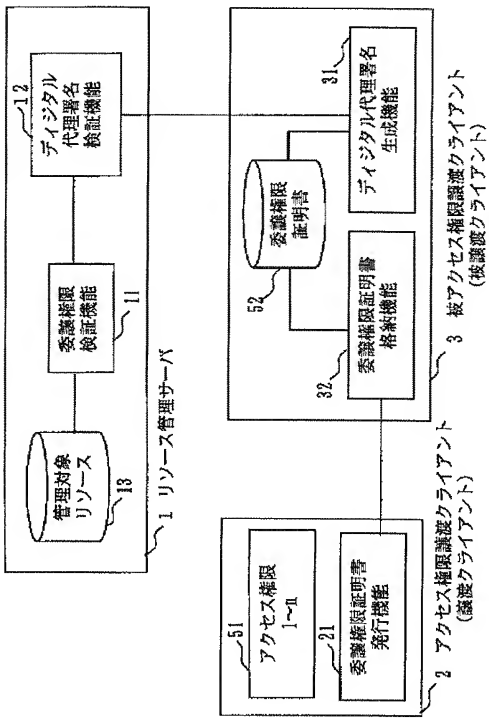
(22)出願日　平成12年11月28日(2000.11.28)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　中野　初美
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　中川路　哲男
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外２名）

Ｆターム(参考)　5B085 AE06 BG07

(54)【発明の名称】　アクセス権限譲渡装置、共有リソース管理システム及びアクセス権限設定方法

(57)【要約】
【課題】　共有リソースへのアクセス権限を持たない装置に対して、一時的なアクセス権限の委譲及び特定種類のアクセス権限の委譲を容易に実現する。
【解決手段】　譲渡クライアント２が、委譲権限証明書発行機能２１を用いて管理対象リソース１３に対するアクセス権限の一時的又は限定的な譲渡を証明する委譲権限証明書５２を発行し、被譲渡クライアント３は、委譲権限証明書格納機能３２を通じて委譲権限証明書５２を取得し、取得した委譲権限証明書５２に基づくアクセス要求であるディジタル代理署名をディジタル代理署名生成機能３１により生成し、リソース管理サーバ１はディジタル代理署名を受け取り、ディジタル代理署名検証機能１２及び委譲権限検証機能１１を通じて、被譲渡クライアント３による管理対象リソースへのアクセスが要求適正であるか否かの検証を行う。



1

【特許請求の範囲】

【請求項１】　共有リソースへのアクセス権限を所有し、前記アクセス権限を有しない無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡することを特徴とするアクセス権限譲渡装置。

【請求項２】　前記アクセス権限譲渡装置は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする請求項１に記載のアクセス権限譲渡装置。

【請求項３】　前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、

前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする請求項１に記載のアクセス権限譲渡装置。

【請求項４】　前記アクセス権限譲渡装置は、

前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有することを特徴とする請求項１に記載のアクセス権限譲渡装置。

【請求項５】　前記アクセス権限譲渡装置は、更に、

前記無権限装置より、前記アクセス権限譲渡証明の発行を要求するアクセス権限譲渡証明発行要求を受け付けるアクセス権限譲渡証明発行要求受付部を有し、

前記アクセス権限譲渡証明発行部は、前記アクセス権限譲渡証明発行要求受付部により受け付けられた前記アクセス権限譲渡証明発行要求に対して前記アクセス権限譲渡証明を発行することを特徴とする請求項４に記載のアクセス権限譲渡装置。

【請求項６】　共有リソースを管理する共有リソース管理装置と、前記共有リソースへのアクセス権限を所有するアクセス権限所有装置と、前記アクセス権限を有しない無権限装置とを有する共有リソース管理システムであって、

前記アクセス権限所有装置は、前記無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡し、

前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、

前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限所有装置により譲渡された前記アクセス権限に従った適正アクセスであるか否かを検証することを特徴とする共有リソース管理システム。

【請求項７】　前記アクセス権限所有装置は、前記無権限装置に対して、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記アクセス権限を譲渡し、

2

前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、

前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限の前記アクセス有効期間の限定に従った適正アクセスであるか否かを検証することを特徴とする請求項６に記載の共有リソース管理システム。

【請求項８】　前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡し、

前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、

前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記特定種類のアクセス権限への限定に従った適正アクセスであるか否かを検証することを特徴とする請求項６に記載の共有リソース管理システム。

【請求項９】　前記アクセス権限所有装置は、

前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有し、

前記無権限装置は、

前記アクセス権限所有装置により発行された前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明と前記共有リソースへのアクセス要求内容とを含むアクセス要求を生成するアクセス要求生成部を有し、

前記共有リソース管理装置は、前記無権限装置により生成された前記アクセス要求を取得し、前記アクセス要求に含まれる前記アクセス要求内容が前記アクセス要求に含まれるアクセス権限譲渡証明に従った適正アクセスであるか否かを検証するアクセス要求検証部を有することを特徴とする請求項６に記載の共有リソース管理システム。

【請求項１０】　前記共有リソース管理システムは、更に、

前記共有リソース管理装置より、前記アクセス要求に含まれる前記アクセス要求内容と前記共有リソース管理装置により検証された前記アクセス要求内容の適正性の検証結果を取得し、取得した前記アクセス要求内容と前記検証結果を記録する監査ログ記録装置を有することを特徴とする請求項９に記載の共有リソース管理システム。

【請求項１１】　前記共有リソース管理システムは、更に、

前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を

前記無権限装置に配布するアクセス権限譲渡証明認証装置を有することを特徴とする請求項１０に記載の共有リソース管理システム。

【請求項１２】　前記共有リソース管理装置は、前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を前記無権限装置に配布することを特徴とする請求項１０に記載の共有リソース管理システム。

【請求項１３】　共有リソースへのアクセス権限を有しない無権限装置に対して、前記アクセス権限の少なくとも一部を設定することを特徴とするアクセス権限設定方法。

【請求項１４】　前記アクセス権限設定方法は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする請求項１３に記載のアクセス権限設定方法。

【請求項１５】　前記共有リソースへの前記アクセス権限は複数種あり、
複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする請求項１３に記載のアクセス権限設定方法。

【請求項１６】　前記アクセス権限設定方法は、
前記無権限装置に対する前記アクセス権限の少なくとも一部の設定を証明するアクセス権限設定証明を発行するアクセス権限設定証明発行ステップを有することを特徴とする請求項１３に記載のアクセス権限設定方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、システムリソースへのアクセス制御をセキュアに行う制御方式に関するものである。

【０００２】

【従来の技術】ワークステーションやパーソナルコンピュータがネットワークに接続され、ハードウェアやソフトウェア、データ等のリソースを相互に共有するような分散ネットワーク環境において、従来よりリソースへの代理アクセス方式が提案されている。たとえば、図１３は従来のリソースへのアクセス方式である。本来のアクセス権をもつノードＡ７００には

・　代理アクセスを要求する代理要求部７２０

・　ノードＡのみが保持する秘密情報を管理する秘密情報管理部７１０がある。

アクセス権を委譲されるノードＢ８００には

・　ノードＡからの代理要求を処理する代理要求受付部８１０

・　ノードＡからの代理要求中にある秘密情報を保持する秘密情報管理部８２０

・　ノードＢのみが保持する秘密情報を管理する秘密情報管理部８４０

・　ノードＡの代わりにリソースにアクセスするための代理実行部８３０

・　ユーザ処理要求の結果を提示する出力手段がある。

アクセスされるリソースを保持するノードＮ９００には

・　ノードＡの秘密情報を管理する秘密情報管理部９１０がある。

【０００３】次に動作について説明する。

【０００４】ノードＡがノードＮにアクセスする場合、次の手順で行われる。

（１）ノードＡの代理要求部７２０が秘密情報管理部７１０で管理されている秘密情報と自ノードの識別子Ａを含む代理要求メッセージを生成し、ノードＢに送付する。

（２）ノードＢの代理要求受付部８１０はノードＡからの代理要求メッセージを受信し、当該メッセージ中の秘密情報を秘密情報管理部８２０に格納する。

（３）代理実行部８３０では、秘密情報管理部８２０よりノードＡの秘密情報を取得し、ノードＮ９００に対する認証用メッセージを生成してノードＮ９００に送付する。

（４）ノードＮ９００は、ノードＡ７００の秘密情報を用いて、認証用メッセージの検証を実施する。

（５）検証に成功すると、ノードＢがノードＮのリソースにアクセス可能となる。

【０００５】

【発明が解決しようとする課題】従来の技術では、リソースへのアクセス権限の譲渡は、譲渡者、被譲渡者、リソース管理者のユーザ認証によって実現されていたため、譲渡する際は全アクセス権を譲渡する。このため、譲渡者の持つ全アクセス権のうち、任意のアクセス権を譲渡することができなかった。また、期限を過ぎた場合のアクセス権限委譲の廃止を実現するには、ユーザ側が期限内か否かを意識しなければならず、ユーザ負担が大きいという問題があった。

【０００６】この発明は上記のような問題点を解決するためになされたもので、リソースへの一時的なのアクセス権限委譲及び特定種類のアクセス権限委譲を容易に実現することを目的とする。

【０００７】

【課題を解決するための手段】この発明に係るアクセス権限譲渡装置は、共有リソースへのアクセス権限を所有し、前記アクセス権限を有しない無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡することを特徴とする。

【０００８】前記アクセス権限譲渡装置は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする。

【０００９】前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡することを特徴とする。

【００１０】前記アクセス権限譲渡装置は、前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有することを特徴とする。

【００１１】前記アクセス権限譲渡装置は、更に、前記無権限装置より、前記アクセス権限譲渡証明の発行を要求するアクセス権限譲渡証明発行要求を受け付けるアクセス権限譲渡証明発行要求受付部を有し、前記アクセス権限譲渡証明発行部は、前記アクセス権限譲渡証明発行要求受付部により受け付けられた前記アクセス権限譲渡証明発行要求に対して前記アクセス権限譲渡証明を発行することを特徴とする。

【００１２】この発明に係る共有リソース管理システムは、共有リソースを管理する共有リソース管理装置と、前記共有リソースへのアクセス権限を所有するアクセス権限所有装置と、前記アクセス権限を有しない無権限装置とを有する共有リソース管理システムであって、前記アクセス権限所有装置は、前記無権限装置に対して、自己の所有する前記アクセス権限の少なくとも一部を譲渡し、前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限所有装置により譲渡された前記アクセス権限に従った適正アクセスであるか否かを検証することを特徴とする。

【００１３】前記アクセス権限所有装置は、前記無権限装置に対して、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記アクセス権限を譲渡し、前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記アクセス権限の前記アクセス有効期間の限定に従った適正アクセスであるか否かを検証することを特徴とする。

【００１４】前記アクセス権限譲渡装置は、前記共有リソースへの複数種のアクセス権限を所有し、前記複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を譲渡し、前記無権限装置は、前記アクセス権限所有装置より譲渡された前記アクセス権限に従って前記共有リソースにアクセスし、前記共有リソース管理装置は、前記無権限装置による前記共有リソースへのアクセスが、前記特定種類のアクセス権限への限定に従った適正アクセスであるか否かを検証することを特徴とする。

【００１５】前記アクセス権限所有装置は、前記無権限装置に対する前記アクセス権限の少なくとも一部の譲渡を証明するアクセス権限譲渡証明を発行するアクセス権限譲渡証明発行部を有し、前記無権限装置は、前記アクセス権限所有装置により発行された前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明と前記共有リソースへのアクセス要求内容とを含むアクセス要求を生成するアクセス要求生成部を有し、前記共有リソース管理装置は、前記無権限装置により生成された前記アクセス要求を取得し、前記アクセス要求に含まれる前記アクセス要求内容が前記アクセス要求に含まれるアクセス権限譲渡証明に従った適正アクセスであるか否かを検証するアクセス要求検証部を有することを特徴とする。

【００１６】前記共有リソース管理システムは、更に、前記共有リソース管理装置より、前記アクセス要求に含まれる前記アクセス要求内容と前記共有リソース管理装置により検証された前記アクセス要求内容の適正性の検証結果を取得し、取得した前記アクセス要求内容と前記検証結果を記録する監査ログ記録装置を有することを特徴とする。

【００１７】前記共有リソース管理システムは、更に、前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を前記無権限装置に配布するアクセス権限譲渡証明認証装置を有することを特徴とする。

【００１８】前記共有リソース管理装置は、前記アクセス権限所有装置より前記アクセス権限譲渡証明を取得し、取得した前記アクセス権限譲渡証明の適正性を判断し、適正と判断されたアクセス権限譲渡証明を前記無権限装置に配布することを特徴とする。

【００１９】この発明に係るアクセス権限設定方法は、共有リソースへのアクセス権限を有しない無権限装置に対して、前記アクセス権限の少なくとも一部を設定することを特徴とする。

【００２０】前記アクセス権限設定方法は、前記無権限装置が前記共有リソースにアクセスできるアクセス有効期間を限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする。

【００２１】前記共有リソースへの前記アクセス権限は複数種あり、複数種のアクセス権限のうち特定種類のアクセス権限に限定して前記無権限装置に対して前記アクセス権限を設定することを特徴とする。

【００２２】前記アクセス権限設定方法は、前記無権限装置に対する前記アクセス権限の少なくとも一部の設定を証明するアクセス権限設定証明を発行するアクセス権限設定証明発行ステップを有することを特徴とする。

【００２３】

【発明の実施の形態】実施の形態１．図１は本発明に係る共有リソース管理システムのブロック構成図である。図において、１は管理対象リソース（共有リソース）１３を管理するリソース管理サーバ（共有リソース管理装置）、２は管理対象リソース１３へのアクセス権限を持つ譲渡クライアント（アクセス権限譲渡装置、アクセス権限所有装置）、３は管理対象リソース１３へのアクセス権限を譲渡クライアント２から譲渡される被譲渡クライアント（無権限装置）である。

【００２４】次に譲渡クライアント２から被譲渡クライアント３に、管理対象リソース１３へのアクセス権限を委譲する際の動作について説明する。譲渡クライアント２は管理対象リソース１３に対して、ｎ個のアクセス種類（５１－１、５１－２、…、５１－ｎ）から構成されているアクセス権限５１を持つ。譲渡クライアント２が被譲渡クライアント３にアクセス種類ｊ、ｋを委譲する場合は、大きく２つの処理に分けられる。委譲権限証明書５２の発行と、委譲権限証明書５２を使って被譲渡クライアント３がリソースアクセスする処理である。

【００２５】ここで、委譲権限証明書５２（アクセス権限譲渡証明）とは、譲渡クライアント２が被譲渡クライアント３に対してアクセス権限を譲渡したことを証明するデータであり、委譲権限証明書５２の例を図２に示す。委譲権限証明書中には、譲渡クライアント、被譲渡クライアント、委譲されるアクセス権限（例ではｊ、ｋ）、委譲有効期限を委譲内容として含み、また委譲内容に対する譲渡者による署名もあわせて記載される。署名は、ＰＫＣＳ（Ｐｕｂｌｉｃ－Ｋｅｙ－Ｃｒｙｐｔｏｇｒａｐｈｙ－Ｓｔａｎｄａｒｄ）＃７に基づいた形式とする。

【００２６】次に、譲渡クライアント２による委譲権限証明書発行の処理ステップを以下にて説明する。

【００２７】（Ｓｔｅｐ　１－１）譲渡クライアント２は委譲権限証明書発行機能（アクセス権限譲渡証明発行部）２１により、被譲渡クライアント３に対して委譲権限証明書５２を発行する。この時、委譲権限証明書中の委譲内容として必要なデータは（１）委譲者を識別する委譲者識別情報（委譲者名等）、（２）被委譲者を識別する被委譲者識別情報（被委譲者名等）、（３）委譲するアクセス種類（ここではｊ、ｋ）、（４）委譲有効期限の４種類である。この委譲内容に対して委譲者の認証書で署名を行う。発行された委譲権限証明書５２は、ネットワークまたはＦＤ等の媒体を介して被譲渡クライアント３に渡される。

（Ｓｔｅｐ　１－２）被譲渡クライアント３は、委譲権限証明書格納機能３２により、受け取った委譲権限証明書５２を格納する。

【００２８】次に、委譲権限証明書を使って、被譲渡クライアント３が管理対象リソース１３をアクセスする場合の処理ステップは次のようになる。

（Ｓｔｅｐ　１－３）被譲渡クライアント３では、ディジタル代理署名生成機能（アクセス要求生成部）３１により、委譲権限証明書５２とリソースへの処理要求（アクセス要求内容）から代理署名内容を生成し、代理署名内容に被譲渡クライアント３が署名した署名データと代理署名内容からディジタル代理署名５３（アクセス要求）を生成する。生成されたディジタル代理署名５３はリソース管理サーバ１に受け渡される。なお、ディジタル代理署名５３の例を図３に示す。ディジタル代理署名５３中には、委譲権限証明書５２、管理対象リソースに対する処理要求を代理署名内容として含み、また代理署名内容に対する被譲渡者による署名もあわせて記載される。

【００２９】（Ｓｔｅｐ　１－４）リソース管理サーバ１のディジタル代理署名検証機能１２では、受け取ったディジタル代理署名５３について（１）被譲渡クライアントの署名の正しさと（２）譲渡クライアントの発行した委譲権限証明書５２中の委譲者による署名の正しさを検証する。検証に成功した場合、ディジタル代理署名検証機能１２は委譲権限検証機能１１にディジタル代理署名５３を受け渡す。

【００３０】（Ｓｔｅｐ　１－５）検証に成功した場合、委譲権限検証機能（アクセス要求検証部）１１では、ディジタル代理署名５３中から処理要求と委譲権限証明書の委譲内容を抽出し、リソース管理サーバが別途保持するアクセスコントロールリストとマッチングをとることによって被譲渡クライアント３が正しくアクセスしているかどうかを検証する。

（Ｓｔｅｐ　１－６）検証に成功した場合のみ、リソースにアクセスを行う。

【００３１】以上のように、委譲者が発行する委譲権限証明書の検証により、被委譲者のリソースアクセスが可能になるため、アクセス権限の一部についての権限委譲（期間限定、アクセス権限の種類の限定）に臨機応変に対応することが可能になる。また、委譲者がアクセス権限の一部の譲渡を証明する委譲権限証明書を発行できるので、一旦委譲された権限の不正利用を防ぐことができる。

【００３２】実施の形態２．以上の実施の形態１では、委譲者が一時的又は限定的な権限委譲を可能にするようにしたものであるが、次に、被委譲者が委譲者に対して、権限委譲を依頼する実施の形態を示す。図４は、このような場合のシステムのブロック構成図である。図において、リソース管理サーバ１は実施の形態１と同様の役割を持つ。

【００３３】次に被譲渡クライアント３からの要求により、譲渡クライアント２から被譲渡クライアント３に、管理対象リソース１３へのアクセス権限を委譲する際の動作について説明する。まず、委譲権限証明書発行の処理ステップは次のようになる。

【００３４】（Ｓｔｅｐ　２－１）被譲渡クライアント３は委譲権限証明書発行申請機能３４により、譲渡クライアント２に対して委譲権限証明書発行申請５６（アクセス権限譲渡証明発行要求）を発行する。図８に示すように、この時、委譲権限証明書発行申請中の申請内容として必要なデータは、（１）委譲者を識別する委譲者識別情報（委譲者名等）、（２）被委譲者を識別する被委譲者識別情報（被委譲者名等）、（３）委譲するアクセス種類（ここではｊ、ｋ）、（４）委譲有効期限の４種類である。この委譲内容に対して被委譲者の認証書で署名を行う。発行された委譲権限証明書発行申請５６は、ネットワークまたはＦＤ等の媒体を介して譲渡クライアント２に渡される。

（Ｓｔｅｐ　２－２）譲渡クライアント２は、委譲権限証明書発行申請検証機能（アクセス権限譲渡証明発行要求受付部）２２により、受け取った委譲権限証明書発行申請５６について申請内容の署名の正しさを検証し、さらにオペレータ等によって申請内容が適切かどうかを判断する。検証に成功した場合、委譲権限証明書発行申請検証機能２２は委譲権限証明書発行機能２１に委譲権限証明書発行申請５６を受け渡す。委譲権限証明書発行機能２１は受け取った委譲権限証明書発行申請５６に基づき委譲権限証明書５２を発行する。被譲渡クライアント３の委譲権限証明証格納機能３２は、譲渡クライアント２の委譲権限証明書発行機能２１より委譲権限証明書５２を受け取り、受け取った委譲権限証明書５２を格納する。

【００３５】委譲権限証明書の発行以降のプロセスは、実施の形態１と同様である。

【００３６】以上のように、被委譲者からの申請を委譲者が判断することによって委譲権限証明書の発行が可能になるため、委譲者からの一方的な委譲ではなく、委譲者／被委譲者双方の委譲要求が実現でき、より柔軟な権限委譲を実現できる。

【００３７】実施の形態３．以上の実施の形態１では、委譲者が一時的又は限定的な権限委譲を可能にするようにしたものであるが、次に、委譲された権限が適切に利用されたかどうかを記録する実施の形態を示す。図５は、このような場合のシステムのブロック構成図である。図において、リソース管理サーバ１、譲渡クライアント２、被譲渡クライアント３は実施の形態１と同様の役割を持つ。４は委譲権限証明書の管理と、委譲権限行使を監査する監査ログを作成する委譲権限サーバである。すなわち、委譲権限サーバ４は、監査ログ記録装置として機能する。

【００３８】次に譲渡クライアント２から被譲渡クライアント３に、管理対象リソース１３へのアクセス権限を委譲する際の動作について説明する。まず、委譲権限証明書発行の処理ステップは次のようになる。

（Ｓｔｅｐ　３－１）実施の形態１と同様に譲渡クライアント２により発行された委譲権限証明書５２は、ネットワークまたはＦＤ等の媒体を介して権限委譲サーバ４に渡される。

（Ｓｔｅｐ　３－２）権限委譲サーバ４は、委譲権限証明書管理機能４１により、受け取った委譲権限証明書５２を格納する。

（Ｓｔｅｐ　３－３）権限委譲サーバ４は、委譲権限証明書配布機能４２により、委譲権限証明書５２を被譲渡クライアント３へ配布する。委譲権限証明書を使って、被譲渡クライアント３が管理対象リソース１３をアクセスする場合の処理ステップは、実施の形態１に記載した（Ｓｔｅｐ　１－３）～（Ｓｔｅｐ　１－５）と同様である。

（Ｓｔｅｐ　３－４）検証に成功した場合のみ、リソースにアクセスを行う。実施の形態１において示したＳｔｅｐ　１－５の検証結果を、権限委譲サーバ４に通知する。

（Ｓｔｅｐ　３－５）権限委譲サーバ４の監査ログ管理機能４３では、Ｓｔｅｐ　３－４において通知された検証結果を監査ログに記述する。権限委譲サーバでは、監査ログによって被譲渡クライアントによるアクセス履歴をチェックできる。

【００３９】監査ログの例を図６に示す。監査ログは、複数の監査ログレコードと、全監査ログレコードに対する委譲権限サーバによる署名で構成される。監査ログレコードには、委譲権限サーバが発行したディジタル代理署名と、被委譲者によって実際に要求された処理、及びその検証結果が記述される。

【００４０】以上のように、委譲権限証明書を権限委譲サーバで一括管理することにより、各委譲クライアントでの委譲権限証明書管理が不要になる。また、委譲した権限の使用状況が、権限委譲サーバに通知されるため、不正なリソース使用の摘発が可能となる。

【００４１】実施の形態４．実施の形態１、３では、委譲クライアントが委譲権限証明書５２を発行したものであるが、次に、権限の委譲の適正性を権限委譲サーバ４で認可し、適正性が認められた後に委譲権限証明書５２を含む権限委譲認可証５８を被譲渡クライアント３に配布する実施の形態を示す。即ち、本実施の形態においては、権限委譲サーバ４は、アクセス権限譲渡証明認証装置として機能する。図７は、このような場合のシステムのブロック構成図である。

【００４２】次に権限委譲サーバ４の認可を得て、譲渡クライアント２から被譲渡クライアント３に、管理対象リソース１３へのアクセス権限を委譲する際の動作について説明する。まず、権限委譲認可証発行の処理ステップは次のようになる。

（Ｓｔｅｐ　４－１）譲渡クライアント２は権限委譲認可証発行要求機能２３により、権限委譲サーバ４に対して権限委譲認可証発行要求５７を発行する。図９に示す

ように、この時、権限委譲認可証発行要求５７に必要なデータは（１）委譲権限証明書、（２）認可者を識別する認可者識別情報（権限委譲サーバ名等）、（３）委譲者による署名の３種類である。発行された権限委譲認可証発行要求５７は、ネットワークまたはＦＤ等の媒体を介して権限委譲サーバ４に渡される。

（Ｓｔｅｐ　４－２）権限委譲サーバ４は、権限委譲認可証発行機能４６により、受け取った権限委譲認可証発行要求５７の譲渡クライアントによる署名を検証する。

（Ｓｔｅｐ　４－３）署名が正しければ、同機能により権限委譲認可証５８を発行する。発行された権限委譲認可証５８は、権限委譲認可証管理機能４７により格納される。なお、図１０に権限委譲認可証５８の例を示す。

（Ｓｔｅｐ　４－４）権限委譲認可証配布機能４８により、権限委譲認可証５８を被譲渡クライアント３へ配布する。

（Ｓｔｅｐ　４－５）被譲渡クライアント３は、権限委譲認可証格納機能３５により、権限委譲認可証５８を格納する。権限委譲認可証５８を使って、被譲渡クライアント３が管理対象リソース１３をアクセスする場合の処理ステップは、次のようになる。

（Ｓｔｅｐ　４－６）権限委譲認可証５８とリソースへの処理要求から、委譲内容を生成し、委譲内容に被譲渡クライアントが署名した署名データと委譲内容からディジタル代理署名５９を生成する。生成されたディジタル代理署名５９はリソース管理サーバ１に受け渡される。なお、図１１にディジタル代理署名５９の例を示す。

（Ｓｔｅｐ　４－７）リソース管理サーバ１のディジタル代理署名検証機能１２では、受け取ったディジタル代理署名５９について（１）被譲渡クライアントの署名の正しさを検証する。検証に成功した場合、ディジタル代理署名検証機能１２は権限委譲認可証検証機能１４にディジタル代理署名５９を受け渡す。

（Ｓｔｅｐ　４－８）権限委譲認可証検証機能１４では、ディジタル代理署名５９から権限委譲認可証５８を抽出し、検証を行う。検証に成功した場合、権限委譲認可証検証機能１４はディジタル代理署名５９を委譲権限検証機能１１に受け渡す。

（Ｓｔｅｐ　４－９）委譲権限検証機能１１では、ディジタル代理署名５９中から処理要求と委譲権限証明書５２の委譲内容を抽出し、リソース管理サーバが別途保持するアクセスコントロールリストとマッチングをとることにより被譲渡クライアント３が正しくアクセスしているかどうかを検証する。

（Ｓｔｅｐ　４－１０）検証に成功した場合のみ、リソースにアクセスを行う。Ｓｔｅｐ　４－９の検証結果を、権限委譲サーバ４に通知する。

（Ｓｔｅｐ　４－１１）権限委譲サーバ４の監査ログ管理機能４３では、Ｓｔｅｐ　４－１０においてリソース管理サーバ１から通知された検証結果を監査ログに記述する。

【００４３】以上のように、委譲権限証明書に対する認可を権限委譲サーバが行うことにより、権限の委譲時におけるなりすましを防止することができる。

【００４４】実施の形態５．実施の形態３、４では、権限委譲サーバが委譲権限行使状態を管理していたものであるが、次に、リソース管理サーバが委譲権限行使状態を管理する実施の形態を示す。図１２は、このような場合のシステムのブロック構成図である。図において、譲渡クライアント２、被譲渡クライアント３は実施の形態４と同様の役割を持つ。リソース管理サーバ１は、実施の形態４の機能に加え、譲渡クライアント２からの権限委譲認可証発行要求５７を処理する権限委譲認可証発行機能１７（権限委譲サーバの４６に相当）、権限委譲認可証管理機能１５（権限委譲サーバの４７に相当）、権限委譲認可証配布機能１６（権限委譲サーバの４８に相当）、監査ログ管理機能１８（権限委譲サーバの４３に相当）を備える。

【００４５】次に譲渡クライアント２の要求により、譲渡クライアント２から被譲渡クライアント３に、管理対象リソース１３へのアクセス権限を委譲する際の動作は、実施の形態３で、権限委譲サーバ４で実施していた処理をリソース管理サーバ１で行ったものと同様なので、割愛する。

【００４６】以上のように、リソース管理サーバが管理対象リソースとともに委譲権限行使状態を一括管理することにより、システム中の構成マシンが削減できる。さらに、委譲した権限の使用状況がリソース管理サーバで認識できるため、監査ログの記録にタイムラグが発生する確率がより微小となり、正確なログが取得できる。

【００４７】これまで説明してきた本発明の特徴をまとめると以下のようになる。リソースへのアクセスの一時的な譲渡を実現することを目的とした、次の構成を備えるシステム。

（ａ）共有リソースを管理するリソース管理サーバ

（ｂ）リソース管理サーバが管理するリソースに対してアクセス権限を持ち、他者にそのアクセス権限を譲渡する権利を持つアクセス権限譲渡クライアント（以下、譲渡クライアント）。

（ｃ）リソース管理サーバが管理するリソースに対してアクセス権限を持たず、譲渡クライアントからアクセス権を譲渡されることによりリソースアクセスが可能になる被アクセス権限譲渡クライアント（以下、被譲渡クライアント）。

上で述べたシステム構成要素は次の機能を備える。

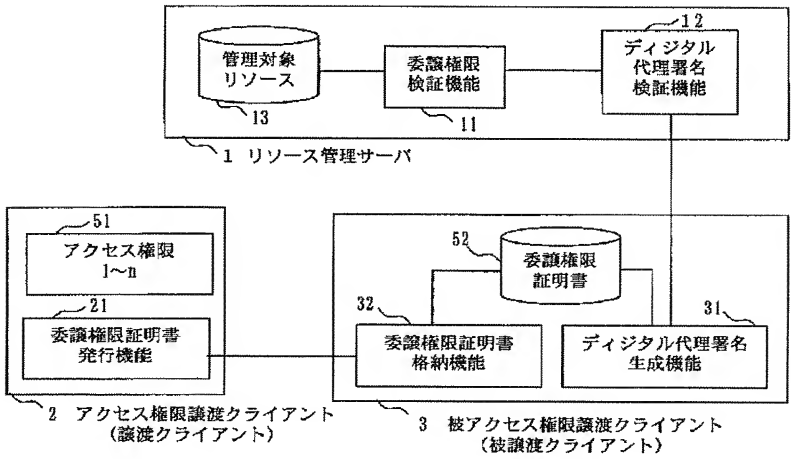
（ａ）譲渡クライアントが、被譲渡クライアントに一時的な譲渡を許可する委譲権限証明書を発行する、委譲権限証明書発行機能

（ｂ）被譲渡クライアントがリソースに対してアクセス要求をする際に送付するディジタル代理署名を作成する

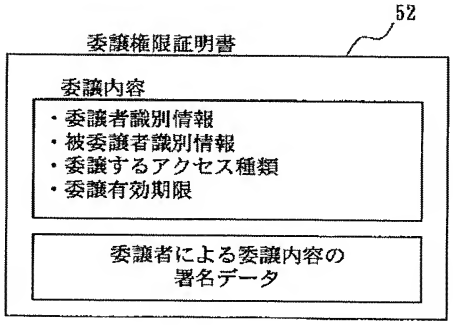
ための、ディジタル代理署名生成機能
（ｃ）被譲渡クライアントが受け取った委譲権限証明書を格納するための、委譲権限証明書格納機能
（ｄ）リソース管理サーバが、被譲渡クライアントが発行したディジタル代理署名を検証するための、ディジタル代理署名検証機能
（ｅ）リソース管理サーバが、被譲渡クライアントがリソースアクセスする際の権限が適切かどうかを検証する委譲権限検証機能
【００４８】更に、以下の構成を追加したシステム。
（ａ）アクセス権限が譲渡された際の、リソースアクセス状況を管理する権限委譲サーバ。
権限委譲サーバは次の機能を備える。
（ａ）権限委譲サーバが権限委譲状況を管理するために委譲権限証明書を管理する委譲権限証明書管理機能
（ｂ）権限委譲サーバが委譲権限証明書を譲渡クライアントから被譲渡クライアントに配布するための委譲権限証明書配布機能
（ｃ）権限委譲サーバが委譲されたリソースへのアクセス権限の実行状況を取得するための監査ログ管理機能
【００４９】更に、以下の機能を備えるシステム。権限委譲サーバによって、権限委譲の認可を行う。
（ａ）譲渡クライアントが、権限委譲サーバに対して、権限委譲認可証の発行を要求するための権限委譲認可証発行要求機能
（ｂ）権限委譲サーバが、譲渡クライアントからの権限委譲認可証の発行要求に対応して、権限委譲認可証を発行するための権限委譲認可証発行機能
（ｃ）権限委譲サーバが、権限委譲認可証を管理、配布する権限委譲認可証管理機能、及び権限委譲認可証配布機能
（ｄ）権限委譲サーバが委譲されたリソースへのアクセス権限の実行状況を取得するための監査ログ管理機能
（ｅ）被譲渡クライアントが、権限委譲サーバから発行された権限委譲認可証を格納するための権限委譲認可証格納機能
（ｆ）リソース管理サーバが、被譲渡クライアントが発行したディジタル代理署名中の権限委譲認可証を検証するための権限委譲認可証検証機能
【００５０】更に、以下の機能を備えるシステム。
（ａ）被譲渡クライアントが、譲渡クライアントに対して、委譲権限証明書の発行を要求するための委譲権限証明書発行申請機能
（ｂ）譲渡クライアントが、被譲渡クライアントからの委譲権限証明書発行申請を検証するための委譲権限証明書発行申請検証機能
【００５１】更に、以下の機能を備えるシステム。
（ａ）譲渡クライアントが、権限委譲サーバに対して、権限委譲認可証の発行を要求するための権限委譲認可証発行要求機能
（ｂ）被譲渡クライアントが、権限委譲サーバから発行された権限委譲認可証を格納するための権限委譲認可証格納機能
（ｃ）リソース管理サーバが、譲渡クライアントからの権限委譲認可証の発行要求に対応して、権限委譲認可証を発行するための権限委譲認可証発行機能
（ｄ）リソース管理サーバが、権限委譲認可証を管理、配布する権限委譲認可証管理機能、及び権限委譲認可証配布機能
（ｅ）リソース管理サーバが、被譲渡クライアントが発行したディジタル代理署名中の権限委譲認可証を検証するための権限委譲認可証検証機能
（ｆ）リソース管理サーバが、委譲されたリソースへのアクセス権限の実行状況を取得するための監査ログ管理機能
【００５２】
【発明の効果】本発明によれば、委譲者が発行する委譲権限証明書の検証により、被委譲者のリソースアクセスが可能になるため、アクセス権限の一部についての権限委譲（期間限定、アクセス権限の種類の限定）に臨機応変に対応することが可能になる。また、委譲者がアクセス権限の一部の譲渡を証明する委譲権限証明書を発行できるので、一旦委譲された権限の不正利用を防ぐことができる。
【００５３】また、本発明によれば、被委譲者からの申請を委譲者が判断することによって委譲権限証明書の発行が可能になるため、委譲者からの一方的な委譲ではなく、委譲者／被委譲者双方の委譲要求が実現でき、より柔軟な権限委譲を実現できる。
【００５４】また、本発明によれば、委譲権限証明書を権限委譲サーバで一括管理することにより、各委譲クライアントでの委譲権限証明書管理が不要になる。また、委譲した権限の使用状況が、権限委譲サーバに通知されるため、不正なリソース使用の摘発が可能となる。
【００５５】更に、本発明によれば、委譲権限証明書に対する認可を権限委譲サーバが行うことにより、権限の委譲時におけるなりすましを防止することができる。
【００５６】また、本発明によれば、リソース管理サーバが管理対象リソースとともに委譲権限行使状態を一括管理することにより、システム中の構成マシンが削減できる。さらに、委譲した権限の使用状況がリソース管理サーバで認識できるため、監査ログの記録にタイムラグが発生する確率がより微小となり、正確なログが取得できる。
【図面の簡単な説明】
【図１】　実施の形態１に係る共有リソース管理システムの構成を示す図。
【図２】　委譲権限証明書の内容を示す図。
【図３】　ディジタル代理署名の内容を示す図。
【図４】　実施の形態２に係る共有リソース管理システ

ムの構成を示す図。
【図５】　実施の形態３に係る共有リソース管理システムの構成を示す図。
【図６】　監査ログの内容を示す図。
【図７】　実施の形態４に係る共有リソース管理システムの構成を示す図。
【図８】　委譲権限証明書発行申請の内容を示す図。
【図９】　権限委譲認可証発行要求の内容を示す図。
【図１０】　権限委譲認可証の内容を示す図。
【図１１】　ディジタル代理署名の内容を示す図。
【図１２】　実施の形態５に係る共有リソース管理システムの構成を示す図。
【図１３】　従来の技術に係るシステムの構成を示す図。
【符号の説明】
１　リソース管理サーバ、２　譲渡クライアント、３　被譲渡クライアント、４　権限委譲サーバ、１１　委譲＊権限検証機能、１２　ディジタル代理署名検証機能、１３　管理対象リソース、１４　権限委譲認可証検証機能、１５　権限委譲認可証管理機能、１６　権限委譲認可証配布機能、１７　権限委譲認可証発行機能、１８　監査ログ管理機能、２１　委譲権限証明書発行機能、２２　委譲権限証明書発行申請検証機能、２３　権限委譲認可証発行要求機能、３１　ディジタル代理署名生成機能、３２　委譲権限証明書格納機能、３４　委譲権限証明書発行申請機能、３５　権限委譲認可証格納機能、４１　委譲権限証明書管理機能、４２　委譲権限証明書配布機能、４３　監査ログ管理機能、４６　権限委譲認可証発行機能、４７　権限委譲認可証管理機能、４８　権限委譲認可証配布機能、５１　アクセス権限、５２　委譲権限証明書、５３　ディジタル代理署名、５４　監査ログ、５６　委譲権限証明書発行申請、５７　権限委譲認可証発行要求、５８　権限委譲認可証。

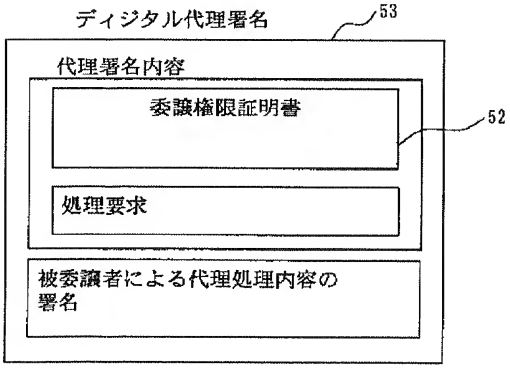
【図１】



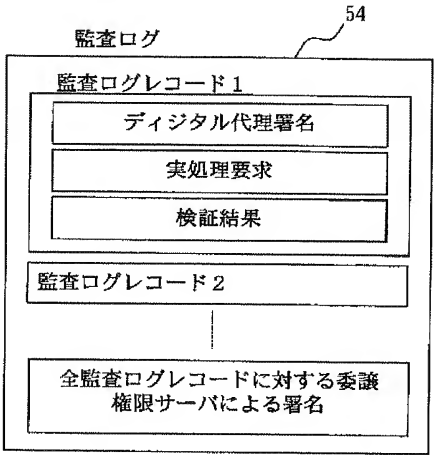
【図２】



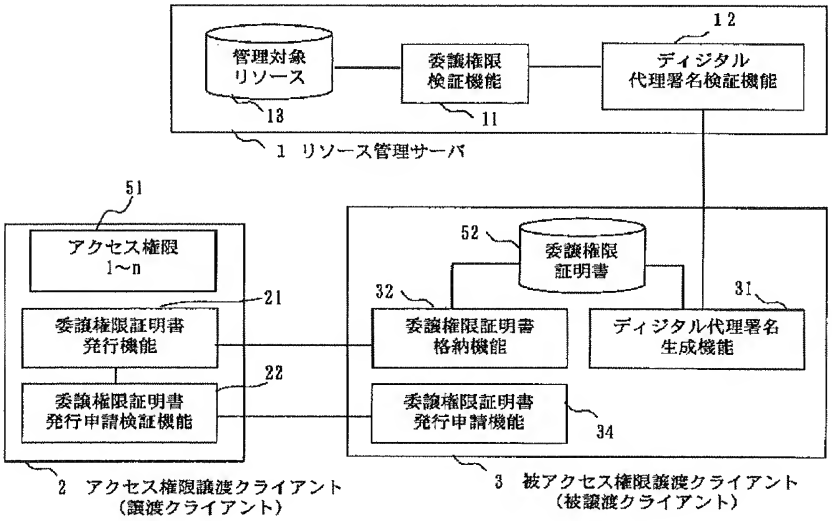
【図３】



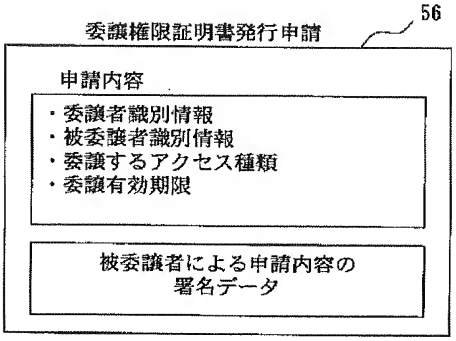
【図６】



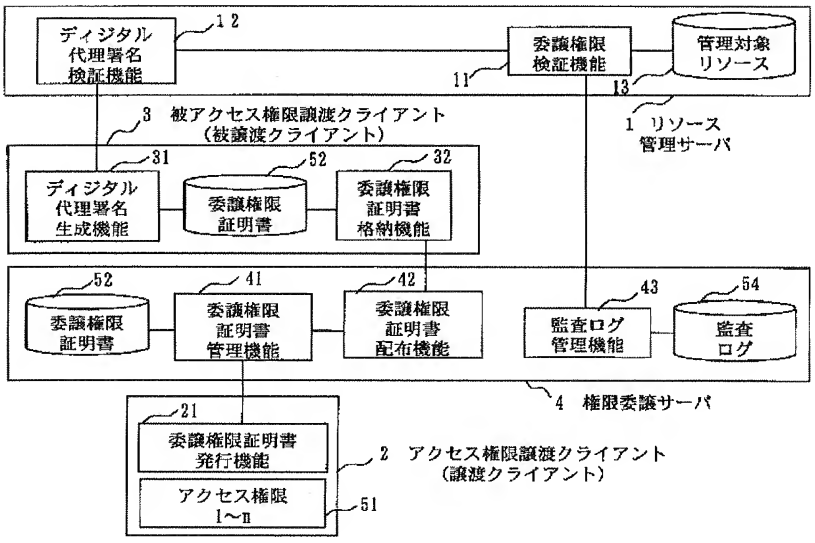
【図４】



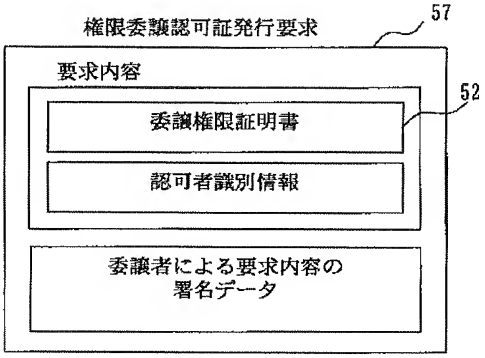
【図８】



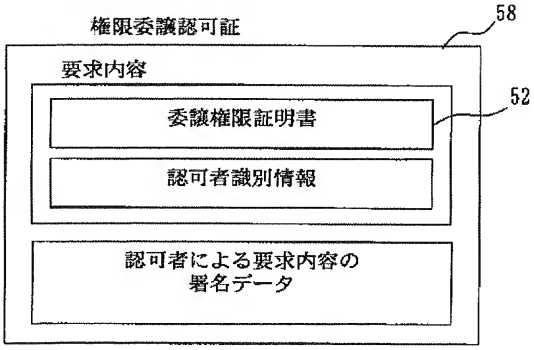
【図５】



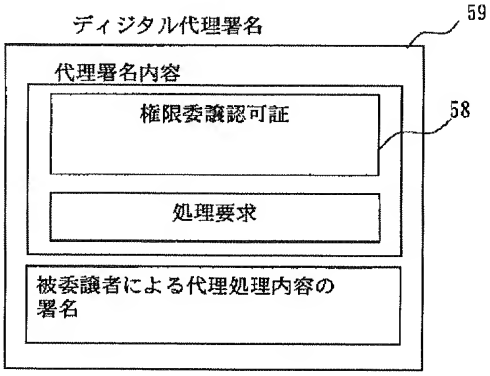
【図９】



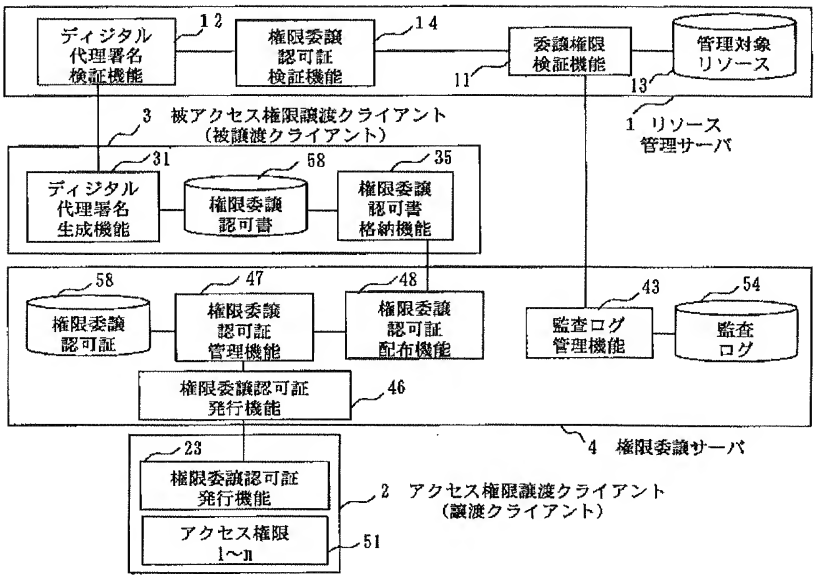
【図１０】



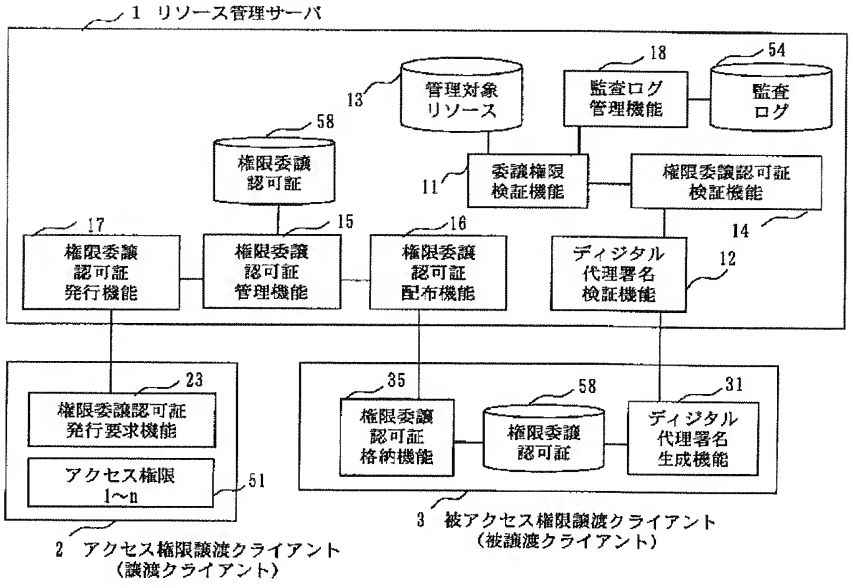
【図１１】



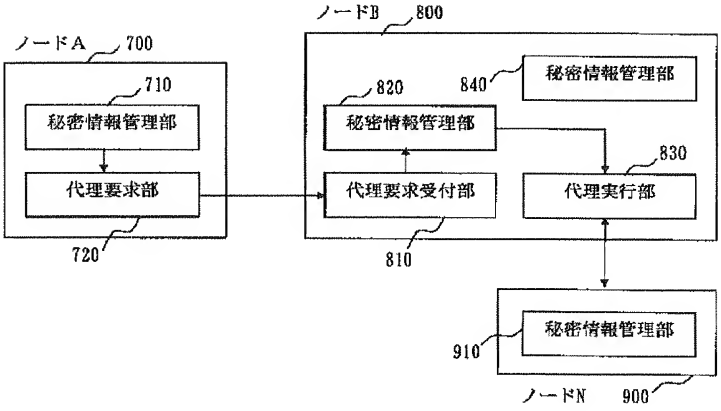
【図７】


ディジタル
代理署名
検証機能
12
権限委譲
認可証
検証機能
14
委譲権限
検証機能
11
管理対象
リソース
13
1 リソース
管理サーバ
3 被アクセス権限譲渡クライアント
（被譲渡クライアント）
31
ディジタル
代理署名
生成機能
58
権限委譲
認可書
35
権限委譲
認可書
格納機能
58
権限委譲
認可証
47
権限委譲
認可証
管理機能
48
権限委譲
認可証
配布機能
43
監査ログ
管理機能
54
監査
ログ
権限委譲認可証
発行機能
46
4 権限委譲サーバ
23
権限委譲認可証
発行機能
アクセス権限
1～n
51
2 アクセス権限譲渡クライアント
（譲渡クライアント）

【図１２】


1 リソース管理サーバ
13
管理対象
リソース
18
監査ログ
管理機能
54
監査
ログ
58
権限委譲
認可証
11
委譲権限
検証機能
権限委譲認可証
検証機能
14
17
権限委譲
認可証
発行機能
15
権限委譲
認可証
管理機能
16
権限委譲
認可証
配布機能
ディジタル
代理署名
検証機能
12
23
権限委譲認可証
発行要求機能
アクセス権限
1～n
51
2 アクセス権限譲渡クライアント
（譲渡クライアント）
35
権限委譲
認可証
格納機能
58
権限委譲
認可証
31
ディジタル
代理署名
生成機能
3 被アクセス権限譲渡クライアント
（被譲渡クライアント）

【図１３】


ノードA
700
710
秘密情報管理部
代理要求部
720
ノードB
800
820
秘密情報管理部
840
秘密情報管理部
830
代理要求受付部
代理実行部
810
910
秘密情報管理部
ノードN
900